UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,728	11/07/2000	Patrick Le Quere	T2147-906625	8212

181 7590 01/24/2007

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
COLIN, CARL G	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/706,728	LE QUERE, PATRICK	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 October 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-18 and 20-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-18 and 20-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 10/30/2006, applicant amends claim 18 to correct minor informalities and cancels claim 19. The following claims 15-18 and 20-34 are presented for examination.

1.1 In response to communications filed on 10/30/2006, the objection to claim 19 has been withdrawn with respect to the amendment.

1.2 Applicant's remarks, pages 8-11, filed on 10/30/2006, with respect to the rejection of claims 15-18 and 20-34 have been fully considered but they are not persuasive. Applicant argues that Dyke does not teach or suggest an input/output module that includes a flash memory and a static random access memory because the second portion cited by the Examiner is distinct from the first portion (see page 9, second paragraph). Examiner respectfully disagrees. The claim limitation reciting "input/output module" has been broadly and reasonably interpreted by the Examiner. The claim merely recites an "input/output module" then "the input/output module includes a microcontroller and memory" (which is apparently a first portion) and the claim further recites "the input/output module further including a flash memory and a static random access memory..." (which is apparently a second portion). Therefore, the CPU PROM and CPU RAM are reasonably interpreted as being also part of the input/output module. Examiner acknowledges that Dyke does not explicitly disclose the processor copying of the flash memory

into the static random access memory during startup. However, IBM Technical Disclosure remedies the deficiency found in Dyke and teaches input/output module including a flash memory and a static random access memory (see diagram) and the advantages of using a flash memory and a static random access memory during startup in an encryption/decryption process. Upon further consideration claims 15-18 and 20-34 remain rejected in view of the prior art.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 15-17, 30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,063,596 to **Dyke** in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5.

As per claim 15, **Dyke** substantially discloses an encryption circuit (1) for simultaneously processing various encryption algorithms, the encryption circuit adapted to be coupled with a

host computer system comprising: an input/output module including a microcontroller and memory, that handles data exchanges between the host system and the circuit via a dedicated bus, for example (see column 3, lines 55-65 and figure 1); an encryption module coupled with the input/output module said encryption module controlling encryption and decryption operations, as well as storage of all sensitive information of the circuit, for example (see column 4, line 65 through column 5, line 14 and column 13, lines 20-30); and isolation means comprising of a dual-port memory between the input/output module and the encryption module, for making the sensitive information stored in the encryption module inaccessible to the host system, for example (see column 4, lines 24-40 and column 2, lines 30-53 and column 14, lines 4-27). **Dyke** discloses a dual-port memory coupled with an input/output module and an encryption module performing parallel processing and a dual-port memory being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output and encryption modules and providing means of isolating the input/output module and the encryption module (see also column 12, lines 4-10 and column 12, lines 40-45). **Dyke** discloses the input/output module further including a flash memory and a static random access memory, the flash memory storing the code for a processor in the microcontroller, (see column 12, lines 29-60). **Dyke** discloses a processor for having access to both RAM and ROM memory during initialization but does not specifically states copying copying contents of the flash memory into the static random access memory (see column 5, lines 5-13 and column 8, lines 10-32). It is obvious to one of ordinary skill in the art that the encryption circuit of Dyke comprises processor adapted for copying contents from flash memory into the static random access memory during startup because data in a flash memory does not

erase during power-off as known in the art. IBM Technical Disclosure Bulletin discloses a single-chip microcontroller comprising flash memory, data RAM memory, and CMOS memory. The ROM stores microcode to be used by a microprocessor and during startup, the microcode is loaded into a RAM because in this way the microcontroller can control the boot-up process and protect the microcode then the microcode can be loaded into the Ram where the code will actually be executed or decryption will take place. Therefore, it would have been obvious to one of ordinary skill in the art of computer security at the time the invention was made to modify Dyke to provide copying contents from flash memory into the static random access memory during startup. One of ordinary skill in the art would have been motivated to do so because it provides a way to protect the microcode and renders control of the boot up process to the microcontroller then the microcode can be loaded into the RAM where the code will actually be executed or decryption will take place if the data is encrypted.

As per claim 16, **Dyke** discloses the claimed circuit of claim 15 and further discloses wherein the isolation means comprises a dual-port memory (see also column 12, lines 4-10 and column 12, lines 40-45).

As per claim 17, **Dyke** discloses the claimed circuit of claim 15 and further discloses a dual-port memory coupled with an input/output module and an encryption module performing parallel processing and a dual-port memory being coupled to a first bus and adapted to simultaneously handle the exchange of data, commands and statuses between the input/output

and encryption modules and providing means of isolating the input/output module and the encryption module (see also column 12, lines 4-10 and column 12, lines 40-45).

As per claim 30, the combined references disclose the claimed circuit of claim 15. **Dyke** discloses a key interface independent of the interface of the link with the host computer that meets the recitation of a serial link, which is independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module, for example (see column 3, line 65 through column 4, line 22). **Dyke** discloses a device capable of preventing linking together of different files in storage (column 2, lines 6-20).

As per claim 32, **Dyke** discloses the limitation of including a card supporting the circuit (column 3, lines 51-53).

3. **Claims 18 and 20-29, 31, and 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,063,596 to **Dyke** in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5 as applied to claims 15-17 and further in view of US Patent 6,021,201 to **Bakhle et al.**

As per claims 18 and 20, both references disclose the claimed encryption circuit of claims 15-17. **Dyke** does not explicitly disclose a CMOS memory which is coupled with the dual-port memory (4) via the first bus of the dual-port memory containing the encryption keys, for example (see column 6, lines 5-21), which is well known in the art. These elements are well

known in the art in a security device and can be implemented by the invention disclosed in Dyke. IBM Technical Disclosure Bulletin supports well known art by disclosing a single-chip microcontroller comprising flash memory, data RAM memory, and CMOS memory. This bulletin further uses a CMOS memory to store security keys because it has the advantage to make probing and examination more difficult in attempt of removal as the CMOS's is sensitive to light and static charge. In addition the RAMs could be backed with a battery when the system was unpowered. Therefore, it would have been obvious to one of ordinary skill in the art of computer security at the time the invention was made to modify the circuit of **Dyke** to provide a CMOS memory coupled with the dual-port memory via the first bus of the dual-port memory containing the encryption keys as taught in IBM Technical Disclosure Bulletin. This modification would have been obvious because one skilled in the art would have been motivated to do so in order to make probing and examination more difficult in attempt of removal and the other advantage would be that the RAMs could be backed with a battery when the system was unpowered.

Both references disclose processing DES algorithm but do not explicitly disclose processing various encryption algorithms. **Bakhle et al** in an analogous art discloses an input/output module including a microcontroller and memory (see figure 1), a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms and being coupled with the first bus of the dual port memory, for example (see column 5, lines 14-67 and figure 3); a second encryption sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled with a first bus of a dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory, performing parallel

processing for example (see column 5, lines 14-67 and see figure 3). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the encryption circuit as combined above to provide a first encryption module and second encryption module for simultaneously performing various encryption algorithms (column 5, lines 14-67) as taught by **Bakhle et al**. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided by **Bakhle et al** to provide a cryptographic device capable of performing cryptographic operations in different formats and while one type of operation is being performed another type can be performed concurrently or in parallel, for instance one cipher processor can operate on data having a first size whereas another processor can operate on a second block size (column 5, lines 14-27 and column 1, lines 32-45).

As per claim 21, **Dyke** teaches isolating means for making keys inaccessible to the host system and isolating means for performing parallel processing (column 12, lines 5-45). **Bakhle et al.** discloses the limitation of an encryption circuit characterized in that the first encryption sub-module comprises an encryption component coupled with the dual-port memory via the first bus of the memory, comprising various encryption automata, respectively dedicated to the processing of symmetric encryption algorithms, and in that the second encryption sub-module comprises at least two encryption processors, respectively dedicated to the processing of asymmetric encryption algorithms, coupled with the encryption module via the internal second bus of the second sub-module, for example (see column 5, lines 14-67 and see figures 3 and 6 with description); and discloses a control unit comprises a security unit that control input and

output and use buses separating from the dual port bus (see figures 3-6 with description and table 2, column 8; column 13, lines 10 et seq.) that meets the recitation of and a bus isolator for isolating the second bus from the first bus of the dual port memory. **Bakhle et al** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). Therefore, claim 21 is rejected on the same rationale as the rejection of claim 18 above.

As per claims 22-23, and 25, **Bakhle et al.** discloses the limitation of an encryption circuit characterized in that one of the two encryption processors is of the CIP type, and in that the other of the two encryption processors is of the ACE type, for example (see column 5, lines 50-67). **Bakhle et al.** discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). Having both processors CIP type is a design choice. Therefore, these claims are rejected on the same rationale as the rejection of claim 18 above.

As per claims 24 and 26, **Bakhle et al.** does not explicitly disclose that one of the processors and the encryption component comprise a FPGA. **Bakhle et al.** discloses input output buffer arrays, for example (see column 9, lines 55 et seq.) and also discloses that the cipher and the hash unit can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms (see end of column 5). It is apparent to one skilled in the art that the units disclosed by **Bakhle et al.** can comprise

FPGA without departing from the spirit and scope of the invention as such unit and component are also well known in the art. Therefore, these claims are rejected on the same rationale as the rejection of claim 18 above.

As per claim 27, the combined references above disclose the claimed circuit of claim 26. **Dyke** also discloses encryption circuit comprises of PROM and SRAM (column 5, lines 1-15).

As per claim 28, the combined references above disclose the claimed circuit of claim 21. **Dyke** further discloses security mechanisms adapted to trigger a reset mechanism of memory (see column 8, lines 25-32 and lines 63-67). IBM bulletin further uses a CMOS memory to store security keys. Therefore, claim 28 is rejected on the same rationale as the rejection of claim 18 above.

As per claim 29, **Dyke** substantially discloses an encryption circuit wherein the microcontroller comprises an input/output processor and a PCI interface for executing the data transfers between the host system and the circuit (column 3, lines 55-67; column 4, lines 8-40). **Bakhle et al** discloses an encryption circuit wherein a microcontroller comprises: an input/output processor and a PCI interface and a flash memory; integrating DMA channels responsible for executing the data transfers between the host system and the circuit, for example (see column 4, lines 26-67 and column 5, lines 34-44);

a flash memory containing the code of the input/output processor and a PCI interface, integrating DMA channels responsible for executing the data transfers between the host system

and the circuit, for example (see column 4, lines 26-67); a flash memory containing the code of the input/output processor , for example (see column 4, lines 38-42); and an SRAM memory that receives a copy of the contents of the flash memory upon startup of the input/output processor, for example (see column 4, lines 26-67). **Bakhle et al** discloses instructions in the memory subsystem for the processors and examples of memory devices and the like that can be implemented with the I/O module, such examples include DRAM, ROM, VRAM and the like. Claim 29 is rejected on the same rationale as the rejection of claim 18 above.

As per claim 31, the combined references disclose the claimed circuit of claim 15. **Dyke** discloses a key interface independent of the interface of the link with the host computer that meets the recitation of a serial link, which is independent of the dedicated PCI bus, said link adapted to be controlled by the encryption module, for example (see column 3, line 65 through column 4, line 22). **Dyke** discloses a device capable of preventing linking together of different files in storage (column 2, lines 6-20). (See also **Bakhle et al,** column 12, line 48 through column 13, line 10). Claim 31 is rejected on the same rationale as the rejection of claim 18 above.

As per claims 33-34, **Dyke** discloses the limitation of including a card supporting the circuit (column 3, lines 51-53).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
January 18, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/19/07